

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor :Keisuke YAMAGUCHI, et al.
Filed :Concurrently herewith
For :SYSTEM AND METHOD FOR...
Serial Number :Concurrently herewith

April 16, 2004

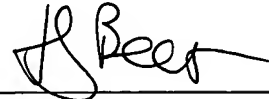
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRIORITY CLAIM AND
SUBMISSION OF PRIORITY DOCUMENT

S I R:

Applicant hereby claims priority under 35 USC 119 from **Japanese** patent application number **2003-113844** filed **April 18, 2003**, a certified copy of which is enclosed.

Respectfully submitted,



Thomas J. Bean
Reg. No. 44,528

Customer Number: 026304
Docket No.: SCEP 21.113



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 4 月 1 8 日
Date of Application:

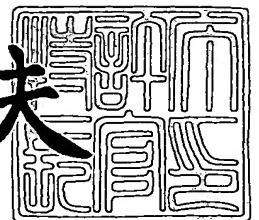
出 願 番 号 特 願 2 0 0 3 - 1 1 3 8 4 4
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 1 1 3 8 4 4]

出 願 人 株式会社ソニー・コンピュータエンタテインメント
Applicant(s):

2 0 0 4 年 1 月 1 6 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



出証番号 出証特 2 0 0 4 - 3 0 0 0 3 9 4

【書類名】 特許願

【整理番号】 SCEI02051

【提出日】 平成15年 4月18日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 19/00

【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 山口 啓介

【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 小巻 賢二郎

【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 増田 勝

【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 島田 宗毅

【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 金江 和広

【発明者】

【住所又は居所】 東京都港区赤坂7丁目1番1号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 木本 陽介

【発明者】

【住所又は居所】 東京都港区赤坂 7 丁目 1 番 1 号 株式会社ソニー・コンピュータエンタテインメント内

【氏名】 神成 真吾

【特許出願人】

【識別番号】 395015319

【氏名又は名称】 株式会社ソニー・コンピュータエンタテインメント

【代理人】

【識別番号】 100105924

【弁理士】

【氏名又は名称】 森下 賢樹

【電話番号】 03-3461-3687

【手数料の表示】

【予納台帳番号】 091329

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信管理システムおよび方法

【特許請求の範囲】

【請求項 1】 ユーザの端末と、
前記端末を認証する認証サーバと、
前記端末をネットワーク上で一意に識別するためのネットワークアドレスを管理する管理サーバと、を備え、
前記端末は、
前記端末を一意に識別可能に割り当てられた、前記端末に固有の機器 ID を保持する保持部と、
前記保持部から前記機器 ID を読み出して前記認証サーバに送り、認証を要求する認証要求部と、
前記認証サーバから認証に成功した旨を証明するための証明書を取得する証明書取得部と、
前記証明書を前記管理サーバに送り、自端末に割り当てられた前記ネットワークアドレスの登録を要求する登録要求部と、を含み、
前記認証サーバは、
前記端末から機器 ID を取得し、認証要求を受け付ける認証受付部と、
前記端末の機器 ID の正当性を認証する認証部と、
前記端末の認証に成功したときに、前記証明書を発行する証明書発行部と、を含み、
前記管理サーバは、
端末を一意に識別する ID とネットワークアドレスを対応づけて保持するデータベースと、
前記端末から前記証明書を取得し、その端末のネットワークアドレスの登録要求を受け付ける登録受付部と、
前記証明書の正当性を検証し、正当であると確認された場合に、その端末の ID とネットワークアドレスを前記データベースに登録する登録部と、
前記端末のネットワークアドレスの照会要求を受け付ける照会受付部と、

照会先の端末の I D をもとに、前記データベースを検索して、その端末のネットワークアドレスを取得する検索部と、

検索結果を回答する回答部と、を含むことを特徴とする通信管理システム。

【請求項 2】 前記保持部は、前記機器 I D を外部から書き換え不能に保持することを特徴とする請求項 1 に記載の通信管理システム。

【請求項 3】 前記認証サーバは、前記端末の認証に成功したときに、その端末を一意に識別する I D を発行する I D 発行部をさらに含み、

前記登録受付部は、前記端末から、前記 I D 発行部がその端末に発行した I D を受け付け、

前記登録部は、前記 I D 発行部がその端末に発行した I D とネットワークアドレスを前記データベースに登録することを特徴とする請求項 1 または 2 に記載の通信管理システム。

【請求項 4】 前記管理サーバは、複数の前記端末を含むグループに関する情報を保持するグループデータベースをさらに含み、

前記照会受付部は、前記グループに関する照会要求を受け付け、

前記検索部は、前記照会要求に基づいて、前記グループデータベースを検索することを特徴とする請求項 1 から 3 のいずれかに記載の通信管理システム。

【請求項 5】 前記管理サーバは、端末間における通信相手のマッチングを管理するマッチング管理部をさらに含み、

前記照会受付部は、前記通信相手に関する条件を受け付け、

前記検索部は、前記条件に基づいて、前記データベースを検索し、

前記マッチング管理部は、検索結果に基づいて、前記通信相手を決定し、

前記回答部は、前記通信相手を回答することを特徴とする請求項 1 から 4 のいずれかに記載の通信管理システム。

【請求項 6】 ユーザの端末が、前記端末内のメモリに保持された、前記端末に固有の機器 I D を読み出すステップと、

前記端末が、前記端末を認証する認証サーバに、前記機器 I D を送信するステップと、

前記認証サーバが、前記機器 I D の正当性を認証するステップと、

認証に成功した場合、前記認証サーバが、認証に成功した旨を証明するための証明書を発行するステップと、

前記認証サーバが、前記証明書を前記端末に送信するステップと、

前記端末が、前記端末をネットワーク上で一意に識別するためのネットワークアドレスを管理する管理サーバに、前記証明書を送信するステップと、

前記管理サーバが、前記証明書を検証するステップと、

前記証明書が正当であると確認された場合、前記管理サーバが、前記端末を一意に識別する ID とネットワークアドレスを対応づけてデータベースに格納するステップと、

を含むことを特徴とする通信管理方法。

【請求項 7】 前記機器 ID を読み出すステップから、前記データベースに格納するステップまでが、ユーザの介在なしに自動的に実行されることを特徴とする請求項 6 に記載の通信管理方法。

【請求項 8】 前記管理サーバが、前記端末のネットワークアドレスの照会要求を受け付けるステップと、

前記管理サーバが、前記端末の ID に基づいて前記データベースを検索し、前記端末のネットワークアドレスを取得するステップと、

前記管理サーバが、前記ネットワークアドレスを回答するステップと、

をさらに含むことを特徴とする請求項 6 または 7 に記載の通信管理方法。

【請求項 9】 自端末を一意に識別可能に割り当てられた、固有の機器 ID を保持する保持部と、

前記保持部から前記機器 ID を読み出して、端末を認証する認証サーバに送り、認証を要求する認証要求部と、

前記認証サーバから認証に成功した旨を証明するための証明書を取得する証明書取得部と、

端末をネットワーク上で一意に識別するためのネットワークアドレスを管理する管理サーバに前記証明書を送り、自端末に割り当てられた前記ネットワークアドレスの登録を要求する登録要求部と、

を備えることを特徴とする端末装置。

【請求項 1 0】 メモリから、自端末を一意に識別可能に割り当てられた、固有の機器 I D を読み出すステップと、

前記端末を認証する認証サーバに、前記機器 I D を送信し、認証を要求するステップと、

前記認証サーバから認証に成功した旨を証明する証明書を取得するステップと、

端末をネットワーク上で一意に識別するためのネットワークアドレスを管理する管理サーバに前記証明書を送信し、自端末に割り当てられたネットワークアドレスの登録を要求するステップと、

を含むことを特徴とする通信管理方法。

【請求項 1 1】 前記登録を要求するステップに先立って、

前記ネットワークへの接続を仲介する接続サーバに、前記ネットワークへの接続を要求するステップと、

前記接続サーバから自端末に付与されたネットワークアドレスを取得するステップと、をさらに含み、

前記登録を要求するステップでは、前記接続サーバから付与されたネットワークアドレスの登録を要求することを特徴とする請求項 1 0 に記載の通信管理方法。

【請求項 1 2】 メモリから、自端末を一意に識別可能に割り当てられた、固有の機器 I D を読み出す機能と、

前記端末を認証する認証サーバに、前記機器 I D を送信し、認証を要求する機能と、

前記認証サーバから認証に成功した旨を証明する証明書を取得する機能と、

端末をネットワーク上で一意に識別するためのネットワークアドレスを管理する管理サーバに前記証明書を送信し、自端末に割り当てられたネットワークアドレスの登録を要求する機能と、

をコンピュータに実現させることを特徴とするコンピュータプログラム。

【請求項 1 3】 メモリから、自端末を一意に識別可能に割り当てられた、固有の機器 I D を読み出す機能と、

前記端末を認証する認証サーバに、前記機器 ID を送信し、認証を要求する機能と、

前記認証サーバから認証に成功した旨を証明する証明書を取得する機能と、

端末をネットワーク上で一意に識別するためのネットワークアドレスを管理する管理サーバに前記証明書を送信し、自端末に割り当てられたネットワークアドレスの登録を要求する機能と、

をコンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 14】 端末を一意に識別する ID と端末のネットワークアドレスを対応づけて保持するデータベースと、

前記端末を認証する認証サーバが発行した、前記端末の認証に成功した旨を証明する証明書を前記端末から取得し、その端末のネットワークアドレスの登録要求を受け付ける登録受付部と、

前記証明書の正当性を検証し、正当であると確認された場合に、その端末の ID とネットワークアドレスを前記データベースに登録する登録部と、

前記端末のネットワークアドレスの照会要求を受け付ける照会受付部と、

照会先の端末の ID をもとに、前記データベースを検索して、その端末のネットワークアドレスを取得する検索部と、

検索結果を回答する回答部と、

を備えることを特徴とする管理サーバ。

【請求項 15】 端末を認証する認証サーバが発行した、前記端末の認証に成功した旨を証明する証明書を前記端末から取得し、その端末のネットワークアドレスの登録要求を受け付けるステップと、

前記証明書の正当性を検証し、正当であると確認された場合に、その端末を一意に識別する ID とその端末のネットワークアドレスをデータベースに登録するステップと、

前記端末のネットワークアドレスの照会要求を受け付けるステップと、

照会先の端末の ID をもとに、前記データベースを検索して、その端末のネットワークアドレスを取得するステップと、

検索結果を回答するステップと、
を含むことを特徴とする通信管理方法。

【請求項 16】 端末を認証する認証サーバが発行した、前記端末の認証に成功した旨を証明する証明書を前記端末から取得し、その端末のネットワークアドレスの登録要求を受け付ける機能と、

前記証明書の正当性を検証し、正当であると確認された場合に、その端末を一意に識別する ID とその端末のネットワークアドレスをデータベースに登録する機能と、

前記端末のネットワークアドレスの照会要求を受け付ける機能と、
照会先の端末の ID をもとに、前記データベースを検索して、その端末のネットワークアドレスを取得する機能と、

検索結果を回答する機能と、
をコンピュータに実現させることを特徴とするコンピュータプログラム。

【請求項 17】 端末を認証する認証サーバが発行した、前記端末の認証に成功した旨を証明する証明書を前記端末から取得し、その端末のネットワークアドレスの登録要求を受け付ける機能と、

前記証明書の正当性を検証し、正当であると確認された場合に、その端末を一意に識別する ID とその端末のネットワークアドレスをデータベースに登録する機能と、

前記端末のネットワークアドレスの照会要求を受け付ける機能と、
照会先の端末の ID をもとに、前記データベースを検索して、その端末のネットワークアドレスを取得する機能と、

検索結果を回答する機能と、
をコンピュータに実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信管理技術に関し、とくに、ネットワークを介した端末間の通信

を管理する技術に関する。

【0 0 0 2】

【従来の技術】

インターネットを利用した通信環境が広く普及し、パーソナルコンピュータなどの端末を用いて、気軽に他のユーザとインターネットを介してコミュニケーションを楽しむことができるようになってきている。ネットワーク接続に対応したゲーム専用機も広く利用されるようになっており、インターネットを介して他のユーザと接続して対戦型ゲームなどを楽しむことができるようになった。

【0 0 0 3】

インターネットにおいては、端末に一意に割り当てられた I P (Internet Protocol) アドレスを用いて、端末を識別して通信を行っている。現状では、多くのユーザは、公衆網を介してインターネットサービスプロバイダ (Internet Service Provider: I S P) に接続し、I S P から I P アドレスを割り当てられ、インターネットに接続している。I S P から割り当てられる I P アドレスは、一般には固定的ではなく、接続のたびに動的に割り当てられる。

【0 0 0 4】

【発明が解決しようとする課題】

特定のユーザの端末と通信するときに、そのユーザの端末に一意的かつ固定的に割り当てられている機器 I D を知っていても、端末に割り当てられた I P アドレスを知らないとインターネットを介して直接通信することができない。I P アドレスが動的に付与される端末と通信する場合は、通信のたびに相手の端末に付与されている I P アドレスを知る必要がある。

【0 0 0 5】

本発明はこうした状況に鑑みてなされたものであり、その目的は、ネットワークを介した端末間の通信の利便性を向上させる技術の提供にある。

【0 0 0 6】

【課題を解決するための手段】

本発明のある態様は、通信管理システムに関する。この通信管理システムは、ユーザの端末と、端末を認証する認証サーバと、端末をネットワーク上で一意に

識別するためのネットワークアドレスを管理する管理サーバと、を備え、端末は、端末を一意に識別可能に割り当てられた、端末に固有の機器IDを保持する保持部と、保持部から機器IDを読み出して認証サーバに送り、認証を要求する認証要求部と、認証サーバから認証に成功した旨を証明するための証明書を取得する証明書取得部と、証明書を管理サーバに送り、自端末に割り当てられたネットワークアドレスの登録を要求する登録要求部と、を含み、認証サーバは、端末から機器IDを取得し、認証要求を受け付ける認証受付部と、端末の機器IDの正当性を認証する認証部と、端末の認証に成功したときに、証明書を発行する証明書発行部と、を含み、管理サーバは、端末を一意に識別するIDとネットワークアドレスを対応づけて保持するデータベースと、端末から証明書を取得し、その端末のネットワークアドレスの登録要求を受け付ける登録受付部と、証明書の正当性を検証し、正当であると確認された場合に、その端末のIDとネットワークアドレスをデータベースに登録する登録部と、端末のネットワークアドレスの照会要求を受け付ける照会受付部と、照会先の端末のIDをもとに、データベースを検索して、その端末のネットワークアドレスを取得する検索部と、検索結果を回答する回答部と、を含む。

【0007】

ネットワークは、たとえば、インターネット、LAN、WANなどであってもよい。ネットワークアドレスは、たとえばインターネットの場合、IPアドレスであってもよい。機器IDは、端末の製造時に、端末内に設けられた外部から書き換え不能なROM (Read Only Memory) に格納されてもよい。

【0008】

認証サーバは、端末の認証に成功したときに、その端末を一意に識別するIDを発行するID発行部をさらに含んでもよい。管理サーバは、複数の端末を含むグループに関する情報を保持するグループデータベースをさらに含み、照会受付部は、グループに関する照会要求を受け付け、検索部は、照会要求に基づいて、グループデータベースを検索してもよい。管理サーバは、端末間における通信相手のマッチングを管理するマッチング管理部をさらに含み、照会受付部は、通信相手に関する条件を受け付け、検索部は、条件に基づいて、データベースを検索

し、マッチング管理部は、検索結果に基づいて、通信相手を決定し、回答部は、通信相手を回答してもよい。

【0 0 0 9】

端末が機器 I D を読み出して認証を要求してから、端末のネットワークアドレスが管理サーバのデータベースに格納されるまでまでの一連の処理が、ユーザの介在なしに自動的に実行されてもよい。

【0 0 1 0】

なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【0 0 1 1】

【発明の実施の形態】

（第 1 の実施の形態）

図 1 は、実施の形態に係る通信管理システム 1 0 の全体構成を示す。通信管理システム 1 0 において、クライアント端末 3 0 0 を認証する認証サーバ 1 0 0 と、クライアント端末 3 0 0 の I P アドレスを管理する管理サーバの一例としてのロケータサーバ 2 0 0 は、それぞれネットワークの一例としてのインターネット 2 0 に接続されている。ユーザが使用するクライアント端末 3 0 0 a および 3 0 0 b は、公衆網 4 0 を介してインターネット 2 0 への接続を仲介するインターネットサービスプロバイダの接続サーバ 3 0 a および 3 0 b に接続され、接続サーバ 3 0 a および 3 0 b を介してインターネット 2 0 に接続されている。

【0 0 1 2】

本実施の形態では、接続サーバ 3 0 a および 3 0 b により I P アドレスが動的に割り当てられるクライアント端末 3 0 0 a および 3 0 0 b の間で、インターネット 2 0 を介した通信を可能とするために、認証サーバ 1 0 0 により認証されたクライアント端末 3 0 0 a の I P アドレスをロケータサーバ 2 0 0 に登録しておく。そして、クライアント端末 3 0 0 b がクライアント端末 3 0 0 a の I P アドレスの照会をロケータサーバ 2 0 0 に要求したときに、ロケータサーバ 2 0 0 はクライアント端末 3 0 0 a の I P アドレスをクライアント端末 3 0 0 b に回答す

る。これにより、クライアント端末 3 0 0 a は、自身に動的に割り当てられている IP アドレスを他のクライアント端末 3 0 0 b に公開することができ、クライアント端末 3 0 0 b は、通信相手のクライアント端末 3 0 0 a に動的に割り当てられている IP アドレスを取得し、クライアント端末 3 0 0 a とインターネット 2 0 を介して通信することができる。

【 0 0 1 3 】

本実施の形態では、認証サーバ 1 0 0 がクライアント端末 3 0 0 を認証するときに、従来のようにクライアント端末 3 0 0 から ID とパスワードの組を受け付けてそれらの正当性を検証するのではなく、クライアント端末 3 0 0 に一意的に割り当てられ、かつ改竄できないように保持された機器 ID を受け付けて、その正当性を検証する。これにより、十分なセキュリティ性を確保しつつ、ID やパスワードを記憶しておかなければならない煩雑さや、認証時の入力の手間から、ユーザを解放することができる。また、この方法によれば、ユーザを介在させる必要がないため、クライアント端末 3 0 0 が自動的に認証サーバ 1 0 0 にアクセスし、認証要求を行うことも可能である。さらに、認証後、ロケータサーバ 2 0 0 に IP アドレスを登録する処理も、同様に自動化することができるので、たとえば、クライアント端末 3 0 0 の起動時、または、クライアント端末 3 0 0 がインターネット 2 0 に接続して IP アドレスが割り当てられた時に、一連の認証処理および登録処理をユーザの介在なしに自動的に行うこともできる。これにより、クライアント端末 3 0 0 がロケータサーバ 2 0 0 に IP アドレスを登録する処理をユーザに意識させることなく完了させることができ、ユーザの利便性をさらに向上させることができる。

【 0 0 1 4 】

上述した認証方法を実現するために、本実施の形態では、ロケータサーバ 2 0 0 に登録可能なクライアント端末 3 0 0 を、認証サーバ 1 0 0 が管理する機器 ID が割り当てられた機器に限定する。すなわち、機器 ID が一意的であること、かつ、改竄できないように保持されていることが保証された機器のみを認証してロケータサーバ 2 0 0 への登録を許可し、機器 ID の一意性および正当性が保証されない機器のロケータサーバ 2 0 0 への登録を拒否する。これにより、ロケー

サーバ 200 に登録されたクライアント端末 300 の ID が重複して IP アドレスを特定できない事態を防ぎ、また、悪意の第三者が他のクライアント端末 300 になりすまして通信を行うことを防止することができる。機器 ID の漏洩や改竄を防ぐために、クライアント端末 300 が認証サーバ 100 に機器 ID を送信するときに機器 ID を暗号化してもよいし、機器 ID に電子署名を付してもよい。これにより、さらにセキュリティ性を向上させることができる。

【0015】

図 2 は、通信管理システム 10 において、クライアント端末 300 a に IP アドレスが付与される手順の概要を示すシーケンス図である。まず、クライアント端末 300 a は、接続サーバ 30 a に対して、インターネット 20 への接続を要求する (S10)。接続サーバ 30 a は、他の端末に割り当てられていない IP アドレスの中から 1 つを選択してクライアント端末 300 a に付与し (S12)、付与した IP アドレスをクライアント端末 300 a に通知する (S14)。クライアント端末 300 a は、付与された IP アドレスによりインターネット 20 を介した通信を行う。接続サーバ 30 a が管理する IP アドレスのうち、いずれがクライアント端末 300 a に付与されるかは、接続のたびに異なるので、クライアント端末 300 a の IP アドレスは接続のたびに変動する。

【0016】

図 3 は、通信管理システム 10 において、クライアント端末 300 a の IP アドレスをロケータサーバ 200 に登録する手順の概要を示すシーケンス図である。まず、クライアント端末 300 a は、自身に固定的に割り当てられている機器 ID を読み出し (S100)、その機器 ID を認証サーバ 100 に送信して、認証を要求する (S102)。機器 ID は、各クライアント端末 300 を一意に識別可能な固有の ID であり、クライアント端末 300 内に設けられた、外部から書き換え不可能な不揮発性メモリに格納され、改竄されないように管理される。認証サーバ 100 は、クライアント端末 300 a から受け付けた機器 ID を認証し (S104)、認証に成功すると、クライアント端末 300 a がロケータサーバ 200 に ID アドレスを登録する際に用いられるチケットと、クライアント端末 300 a を一意に識別する ID (以下、「ロケータ ID」と呼ぶ) を発行して

(S106)、クライアント端末300aに送信する(S108)。このチケットは、端末の認証が成功したことを証明するための証明書であり、不正に偽造されないように、たとえば、認証サーバ100の電子署名が付加されてもよい。また、第三者に漏洩することを防ぐために、たとえば、ロケータサーバ200の公開鍵により暗号化されてもよい。ロケータIDは、ロケータサーバ200において、クライアント端末300を一意に識別するために用いられる。ロケータIDは、機器IDを所定の規則にしたがって翻訳したものであってもよく、同一のクライアント端末300には、同一のロケータIDが固定的に発行されてもよい。

【0017】

ロケータサーバ200においてクライアント端末300を識別するために、機器IDを用いてもよいが、機器IDは、クライアント端末300の認証に用いる極めて重要な情報であるから、本実施の形態では、機器IDをロケータサーバ200に通知することを避け、ロケータサーバ200においては、認証サーバ100が発行したロケータIDによりクライアント端末300を識別する。これにより、機器IDの漏洩の危険性を最小限に抑えることができる。

【0018】

クライアント端末300aは、認証サーバ100からチケットを受け取ると、そのチケットと自身に割り当てられたIPアドレスをロケータサーバ200に送信して、IPアドレスの登録を要求する(S110)。ロケータサーバ200には、クライアント端末300aのロケータIDおよびIPアドレスと、それらの正当性を示す情報が送信されればよいが、ここでは、クライアント端末300aのロケータIDはチケットに含まれているものとする。ロケータサーバ200は、クライアント端末300aから受け付けたチケットの正当性を検証し(S112)、正当であることが確認されると、クライアント端末300aのロケータIDとIPアドレスを対応づけて登録し(S114)、登録が行われた旨をクライアント端末300aに応答する(S116)。前述したように、これらの一連の手順は、途中でユーザからの指示を介することなく、クライアント端末300aにより自動的に行われてもよい。

【0019】

図4は、通信管理システム10において、クライアント端末300aのIPアドレスをロケータサーバ200に照会する手順の概要を示すシーケンス図である。照会元のクライアント端末300bは、ロケータサーバ200に、照会先のクライアント端末300aのロケータIDを送信して、そのクライアント端末300aのIPアドレスの照会を要求する(S200)。ロケータサーバ200は、クライアント端末300bから受け付けたクライアント端末300aのロケータIDをもとに、そのクライアント端末300aのIPアドレスを検索し(S202)、検索結果をクライアント端末300bに回答する(S204)。これにより、クライアント端末300bは、通信相手のクライアント端末300aのロケータIDを記憶しておけば、クライアント端末300aのIPアドレスが動的に変化しても、IPアドレスを知ることができるので、インターネット20を介して通信を行うことができる。

【0020】

図5は、認証サーバ100の内部構成を示す。この構成は、ハードウェア的には、任意のコンピュータのCPU、メモリ、その他のLSIで実現でき、ソフトウェア的にはメモリにロードされたプログラムなどによって実現されるが、ここではそれらの連携によって実現される機能ブロックを描いている。したがって、これらの機能ブロックがハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できることは、当業者には理解されるところである。認証サーバ100は、通信制御部102、認証要求受付部110、認証部120、チケット発行部130、および端末データベース140を含む。

【0021】

通信制御部102は、インターネット20を介した他の装置との通信を制御する。端末データベース140は、認証すべきクライアント端末300の機器IDを保持する。この端末データベース140は、クライアント端末300の製造主体、すなわち、クライアント端末300に機器IDを付与した主体から入手してもよい。認証要求受付部110は、クライアント端末300から認証要求を受け付ける。このとき、認証要求受付部110は、要求元のクライアント端末300の機器IDを取得する。認証部120は、取得した機器IDが本通信管理システ

ム 10 によるサービスを楽しむクライアント端末 300 の機器 ID であるかを端末データベース 140 を参照して認証する。認証に失敗した場合は、通信制御部 102 を介して、認証に失敗した旨をクライアント端末 300 に応答する。認証に成功した場合は、チケット発行部 130 が、認証されたことを証明するためのチケットと、ロケータ ID を発行する。すなわち、チケット発行部 130 は、ID 発行部の機能を兼ねる。発行されたチケットとロケータ ID は、通信制御部 102 を介して、クライアント端末 300 に送信される。

【0022】

図 6 は、ロケータサーバ 200 の内部構成を示す。この構成も、ハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できる。ロケータサーバ 200 は、通信制御部 202、登録受付部 210、登録部 212、応答部 214、管理部 220、クエリ受付部 230、検索部 232、回答部 234、およびユーザデータベース 242 を記憶する記憶部 240 を含む。

【0023】

通信制御部 202 は、インターネット 20 を介した他の装置との通信を制御する。ユーザデータベース 242 は、ロケータサーバ 200 に登録されたクライアント端末 300 に関する情報を保持する。図 7 は、ユーザデータベース 242 の内部データの一例を示す。ユーザデータベース 242 には、ロケータ ID 欄 400、IP アドレス欄 402、および登録日時欄 404 が設けられており、クライアント端末 300 のロケータ ID と IP アドレスを対応づけて保持する。登録日時欄 404 は、後述するように、登録された IP アドレスの有効期限を管理するために用いられる。

【0024】

登録受付部 210 は、クライアント端末 300 から IP アドレスの登録要求を受け付ける。このとき、登録受付部 210 は、要求元のクライアント端末 300 のロケータ ID とチケットを取得する。登録部 212 は、取得したチケットの正当性を検証し、チケットの正当性が確認された場合は、要求元のクライアント端末 300 のロケータ ID と IP アドレスを対応づけてユーザデータベース 242 に登録し、応答部 214 は、登録に成功した旨をクライアント端末 300 に応答

する。チケットの正当性が確認できなかった場合は、応答部 2 1 4 は、登録に失敗した旨をクライアント端末 3 0 0 に応答する。

【 0 0 2 5 】

クエリ受付部 2 3 0 は、クライアント端末 3 0 0 から IP アドレスの照会要求を受け付ける。このとき、クエリ受付部 2 3 0 は、照会先のクライアント端末 3 0 0 のロケータ ID を取得する。検索部 2 3 2 は、照会先のクライアント端末 3 0 0 のロケータ ID をユーザデータベース 2 4 2 から検索し、そのクライアント端末 3 0 0 に現在割り当てられている IP アドレスを取得する。このとき、登録日時欄 4 0 4 を参照して、登録されてから所定の期間以上更新されていないクライアント端末 3 0 0 は、既にインターネット 2 0 への接続を切断している可能性があるため、その IP アドレスは無効であると判断してもよい。回答部 2 3 4 は、検索部 2 3 2 による検索結果をクライアント端末 3 0 0 に回答する。

【 0 0 2 6 】

クエリ受付部 2 3 0 は、クライアント端末 3 0 0 がインターネット 2 0 に接続中であるか否かの照会を受け付けてもよい。このとき、検索部 2 3 2 は、そのクライアント端末 3 0 0 のロケータ ID がユーザデータベース 2 4 2 に登録されているか否かを検索し、登録されていれば、回答部 2 3 4 は、そのクライアント端末 3 0 0 がオンラインである旨を回答し、登録されていなければ、回答部 2 3 4 は、そのクライアント端末 3 0 0 がオフラインである旨を回答する。

【 0 0 2 7 】

管理部 2 2 0 は、ユーザデータベース 2 4 2 に登録された IP アドレスの有効期限を管理する。ユーザデータベース 2 4 2 に登録されているクライアント端末 3 0 0 が、電源の切断などによりインターネット 2 0 への接続を切断した後、ユーザデータベース 2 4 2 にそのクライアント端末 3 0 0 の情報が残ったままになっていると、誤った情報を他のクライアント端末 3 0 0 に回答してしまうことになる。このような事態を回避するために、たとえば、クライアント端末 3 0 0 がインターネット 2 0 に接続している間、所定の間隔で繰り返しロケータサーバ 2 0 0 に登録させるようにしてもよい。この場合、管理部 2 2 0 は、ユーザデータベース 2 4 2 の登録日時欄 4 0 4 を参照し、所定の期間以上更新されていないク

クライアント端末 3 0 0 のレコードを削除する。管理部 2 2 0 が、登録日時から所定の期間が経過したクライアント端末 3 0 0 に対して、インターネット 2 0 に接続しているか、登録されている IP アドレスから変更されていないかを問い合わせてもよい。

【 0 0 2 8 】

図 8 は、クライアント端末 3 0 0 の内部構成を示す。この構成も、ハードウェアのみ、ソフトウェアのみ、またはそれらの組合せによっていろいろな形で実現できる。クライアント端末 3 0 0 は、通信制御部 3 0 2、認証要求部 3 1 0、チケット取得部 3 1 2、登録要求部 3 1 4、クエリ要求部 3 2 0、回答取得部 3 2 2、通信部 3 3 0、および機器 ID 保持部 3 4 0 を含む。

【 0 0 2 9 】

通信制御部 3 0 2 は、インターネット 2 0 を介した他の装置との通信を制御する。通信制御部 3 0 2 は、インターネット 2 0 に接続するために、公衆網 4 0 を介して接続サーバ 3 0 に接続要求を送り、接続サーバ 3 0 から付与された IP アドレスを取得する。以降、通信制御部 3 0 2 は、この IP アドレスを用いて、インターネット 2 0 を介した通信を行う。機器 ID 保持部 3 4 0 は、外部から書き換え不可能な ROM などの不揮発性メモリであり、各クライアント端末 3 0 0 を一意に識別可能な固有の機器 ID を保持する。機器 ID は、クライアント端末 3 0 0 の製造時に機器 ID 保持部 3 4 0 に書き込まれ、以降は改竄されないように管理される。

【 0 0 3 0 】

認証要求部 3 1 0 は、機器 ID 保持部 3 4 0 から自身の機器 ID を読み出し、その機器 ID を認証サーバ 1 0 0 に送って、認証を要求する。チケット取得部 3 1 2 は、認証サーバ 1 0 0 がクライアント端末 3 0 0 を認証したときに発行するチケットと、認証サーバ 1 0 0 により発行されたロケータ ID を取得する。登録要求部 3 1 4 は、取得したチケットをロケータサーバ 2 0 0 に送って、自身の IP アドレスの登録を要求する。

【 0 0 3 1 】

クエリ要求部 3 2 0 は、他のクライアント端末 3 0 0 とインターネット 2 0 を

介して通信を行う前に、そのクライアント端末300のIPアドレスを知るために、ロケータサーバ200に照会を要求する。クエリ要求部320は、他のクライアント端末300のオンライン状況をロケータサーバ200に照会してもよい。回答取得部322は、ロケータサーバ200から回答を取得する。通信部330は、ロケータサーバ200から取得した通信先のクライアント端末300のIPアドレスを用いて、そのクライアント端末300と通信を行う。これにより、クライアント端末300間でインターネット20を介した通信が可能となり、たとえば、IP電話や、ネットワーク対戦型ゲームなどを実現することができる。

【0032】

以上、説明したように、本実施の形態の通信管理システム10によれば、クライアント端末300のIPアドレスが変動する場合であっても、通信相手のクライアント端末300のIPアドレスを取得し、インターネット20を介して通信を行うことができる。本通信管理システム10を、クライアント端末300の製造主体が運営する場合は、全てのクライアント端末300の機器IDを管理することができるので、全てのクライアント端末300のIPアドレスを統括して登録し、照会を受け付けることができる。これにより、端末間通信を利用したゲームなどのサービスの提供主体が、個別に本実施の形態の通信管理システム10を用意する必要がなくなるので、ユーザにとっても、サービス提供主体にとっても、メリットが大きい。

【0033】

認証サーバ100は、機器IDの機密性を保証する観点から、クライアント端末300の製造主体が運営するのが好ましいが、ロケータサーバ200は、サービス提供主体により運営されてもよく、複数のサービス提供主体により複数のロケータサーバ200が設けられてもよい。認証サーバ100は、機器IDの漏洩を防止するために、極めて高いセキュリティ性が要求されるが、上述したように、ロケータサーバ200には機器IDは通知されず、ロケータIDによりクライアント端末300が識別されるので、認証サーバ100に比べると、低いセキュリティレベルでロケータサーバ200を運用してもよい。これにより、ロケータサーバ200の設置、運用に要するコストを抑えることができる。また、不特定

多数のクライアント端末300からのクエリ要求を受け付けるべきロケータサーバ200を、認証サーバ100とは別に設けておくことで、認証サーバ100のセキュリティ性を向上させ、機器IDの漏洩を防止することができる。

【0034】

(第2の実施の形態)

本実施の形態では、複数のユーザをグループ化して管理することが可能な通信管理システム10について説明する。本実施の形態の通信管理システム10の全体構成は、図1に示した第1の実施の形態の通信管理システム10と同様である。また、本実施の形態の認証サーバ100およびクライアント端末300の内部構成は、それぞれ、図5、図8に示した第1の実施の形態のものと同様である。

【0035】

図9は、本実施の形態のロケータサーバ200の内部構成を示す。本実施の形態のロケータサーバ200は、図6に示した第1の実施の形態のロケータサーバ200の構成に加えて、グループデータベース244を備える。その他の構成は、第1の実施の形態と同様であり、同様の構成には同じ符号を付している。以下、第1の実施の形態と異なる点を中心に説明する。

【0036】

図10は、本実施の形態のユーザデータベース242の内部データの一例を示す。本実施の形態のユーザデータベース242には、図7に示した第1の実施の形態のユーザデータベース242の内部データに加えて、グループID欄408が設けられている。グループID欄408は、そのユーザが属するグループのIDを格納する。図11は、グループデータベース244の内部データの一例を示す。グループデータベース244には、グループID欄420、メンバ数欄422、およびロケータID欄424が設けられている。メンバ数欄422は、そのグループを構成するメンバの数を格納する。ロケータID欄424は、メンバの数だけ設けられ、そのグループを構成するメンバのクライアント端末300のロケータIDを格納する。

【0037】

登録受付部210は、クライアント端末300から登録を受け付けるときに、

そのユーザが属するグループの情報をさらに取得し、登録部 2 1 2 は、ユーザデータベース 2 4 2 およびグループデータベース 2 4 4 に受け付けた情報を登録する。グループが未登録の場合は、登録部 2 1 2 は、グループデータベース 2 4 4 にそのグループを新規登録する。クエリ受付部 2 3 0 は、グループに関する照会要求を受け付ける。たとえば、グループ ID 「0 0 0 1」のグループに属するメンバーの IP アドレスの照会を受け付けると、検索部 2 3 2 は、まずグループデータベース 2 4 4 を検索して、グループ ID 「0 0 0 1」のグループに属するメンバーのロケータ ID を取得し、さらにユーザデータベース 2 4 2 を検索して、個々のメンバーの IP アドレスを取得する。回答部 2 3 4 は、各メンバーの IP アドレスを回答する。以上の構成により、ユーザをグループ化して管理することが可能となる。

【0 0 3 8】

(第 3 の実施の形態)

本実施の形態では、端末間における通信相手をマッチングすることが可能な通信管理システム 1 0 について説明する。本実施の形態の通信管理システム 1 0 の全体構成は、図 1 に示した第 1 の実施の形態の通信管理システム 1 0 と同様である。また、本実施の形態の認証サーバ 1 0 0 およびクライアント端末 3 0 0 の内部構成は、それぞれ、図 5、図 8 に示した第 1 の実施の形態のものと同様である。

【0 0 3 9】

図 1 2 は、本実施の形態のロケータサーバ 2 0 0 の内部構成を示す。本実施の形態のロケータサーバ 2 0 0 は、図 6 に示した第 1 の実施の形態のロケータサーバ 2 0 0 の構成に加えて、マッチング管理部 2 3 6 を備える。その他の構成は、第 1 の実施の形態と同様であり、同様の構成には同じ符号を付している。以下、第 1 の実施の形態と異なる点を中心に説明する。

【0 0 4 0】

図 1 3 は、本実施の形態のユーザデータベース 2 4 2 の内部データの一例を示す。本実施の形態のユーザデータベース 2 4 2 は、図 7 に示した第 1 の実施の形態のユーザデータベース 2 4 2 の内部データに加えて、メディア ID 欄 4 0 6、

コミュニティ・フラグ欄 410、ニックネーム欄 412、およびネットワークモード欄 414 が設けられている。メディア ID 欄 406 は、クライアント端末 300 に接続されている記録媒体に付与された固有な ID を格納する。たとえば、クライアント端末 300 がゲーム装置である場合、メディア ID によりユーザが実行中のゲームの種類を知ることができる。メディア ID に代えて、ユーザが起動中のアプリケーションの種類などを識別するための情報が格納されてもよい。

【0041】

コミュニティ・フラグ欄 410 は、ユーザが通信相手を求めているか否か、通信相手を求めている場合は、ユーザ自身の情報や、希望する通信相手の種別などの情報を格納する。通信相手の種別に関する情報は、たとえば、ゲーム、チャット、電話など、通信用のアプリケーションの種類、通信相手の年齢、性別などの属性、ゲームの場合は、対戦相手のレベルなどであってもよい。コミュニティ・フラグ欄 410 は、サービス提供主体が任意に利用できるようにしてもよい。これにより、より柔軟性を有するシステムを構築することができる。

【0042】

ニックネーム欄 412 は、ユーザのニックネームを格納する。ユーザのニックネームは、ユーザのクライアント端末 300 がロケータサーバ 200 に登録を要求したときに、ユーザから受け付けてもよい。クライアント端末 300 が、通信相手のクライアント端末 300 のロケータ ID を記憶する際に、ユーザのニックネームを対応づけて記憶することで、より分かりやすく、フレンドリーなニックネームにより通信相手の情報を管理することができる。

【0043】

ネットワークモード欄 414 は、クライアント端末 300 のネットワーク状態、たとえば、直接通信が可能であるか否かなどの情報を格納する。たとえば、複数人で対戦を行おうとしている 2 人のユーザが、双方とも直接通信が不可能な状態にあった場合、外部からの直接通信が可能な他のユーザを検索して対戦を行う、などといった利用法が考えられる。

【0044】

ユーザデータベース 242 は、さらに、ユーザの属性など、通信相手のマッチ

ングに必要な情報を格納する欄を有してもよい。ユーザの属性などの個人情報、予めロケータサーバ200に登録しておき、ユーザデータベース242に保持されてもよい。

【0045】

登録受付部210は、クライアント端末300から登録を受け付けるときに、そのクライアント端末300に接続されている記録媒体のメディアIDと、マッチングに関する要望などを受け付ける。クライアント端末300の認証要求部310は、自身に接続されている記録媒体のメディアIDを読み出して登録受付部210に提供する。登録部212は、受け付けた情報をユーザデータベース242に格納する。クエリ受付部230は、クライアント端末300から、マッチング要求を受け付ける。たとえば、対戦を希望するゲームの種類、通信用のアプリケーションの種類、通信相手の種別に関する希望などの条件を受け付ける。検索部232は、受け付けた条件に基づいて、ユーザデータベース242から、該当するユーザのクライアント端末300を検索する。マッチング管理部236は、検索結果に基づいて通信相手をマッチングする。回答部234は、マッチングされた通信相手をクライアント端末300に回答する。以上の構成により、ユーザは、希望する通信相手を自動的に見つけ出し、通信を行うことができる。

【0046】

以上、本発明を実施の形態をもとに説明した。この実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【0047】

【発明の効果】

本発明によれば、ネットワークを介した端末間の通信の利便性を向上させる技術を提供することができる。

【図面の簡単な説明】

【図1】 第1の実施の形態に係る通信管理システムの全体構成を示す図である。

【図 2】 通信管理システムにおいて、クライアント端末に I P アドレスが付与される手順の概要を示すシーケンス図である。

【図 3】 通信管理システムにおいて、クライアント端末の I P アドレスをロケータサーバに登録する手順の概要を示すシーケンス図である。

【図 4】 通信管理システムにおいて、クライアント端末の I P アドレスをロケータサーバに照会する手順の概要を示すシーケンス図である。

【図 5】 第 1 の実施の形態に係る認証サーバの内部構成を示す図である。

【図 6】 第 1 の実施の形態に係るロケータサーバの内部構成を示す図である。

【図 7】 第 1 の実施の形態に係るユーザデータベースの内部データの一例を示す図である。

【図 8】 第 1 の実施の形態に係るクライアント端末の内部構成を示す図である。

【図 9】 第 2 の実施の形態に係るロケータサーバの内部構成を示す図である。

【図 1 0】 第 2 の実施の形態に係るユーザデータベースの内部データの一例を示す図である。

【図 1 1】 第 2 の実施の形態に係るグループデータベースの内部データの一例を示す図である。

【図 1 2】 第 3 の実施の形態に係るロケータサーバの内部構成を示す図である。

【図 1 3】 第 3 の実施の形態に係るユーザデータベースの内部データの一例を示す図である。

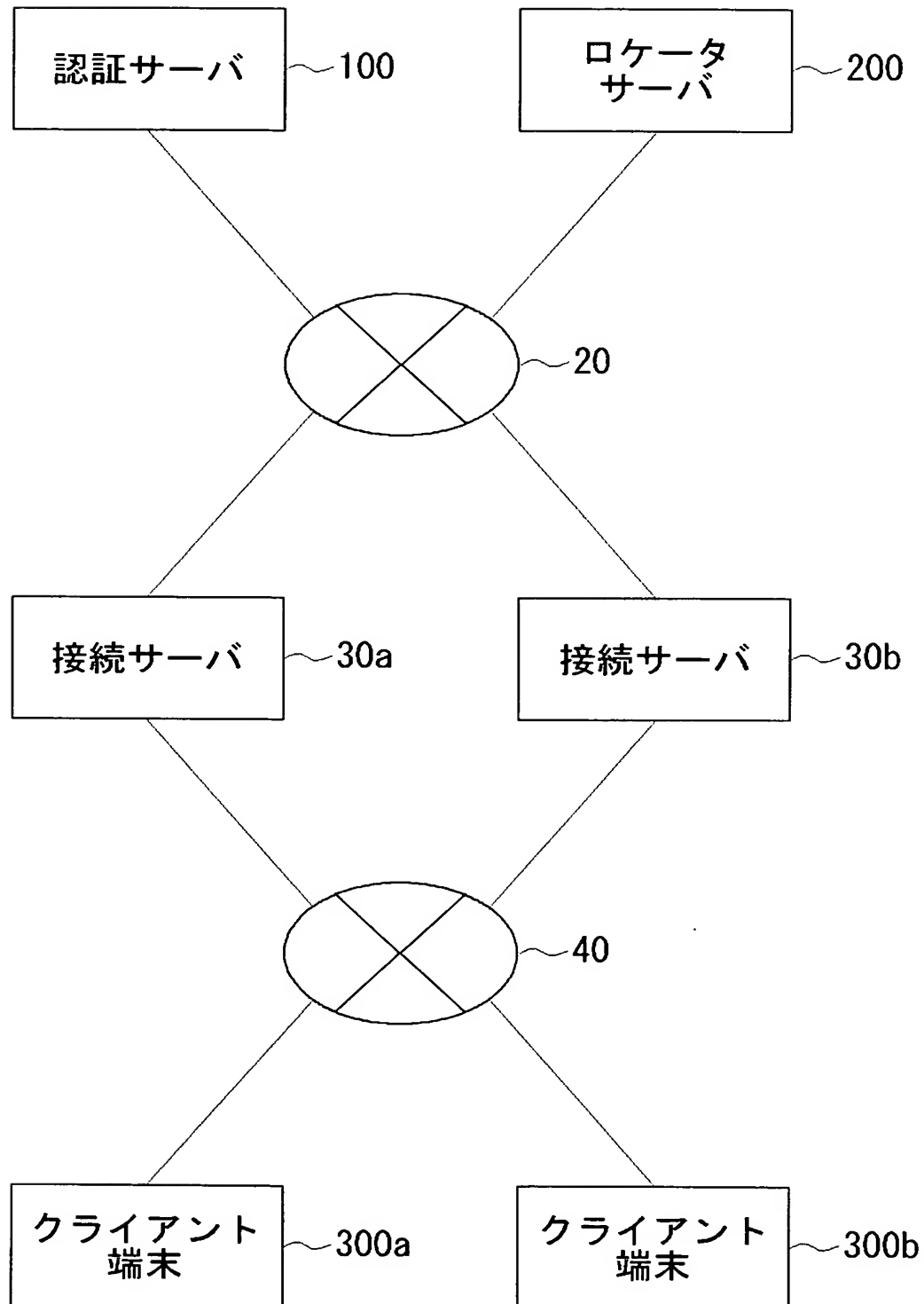
【符号の説明】

1 0 . . . 通信管理システム、3 0 . . . 接続サーバ、1 0 0 . . . 認証サーバ、1 1 0 . . . 認証要求受付部、1 2 0 . . . 認証部、1 3 0 . . . チケット発行部、1 4 0 . . . 端末データベース、2 0 0 . . . ロケータサーバ、2 1 0 . . . 登録受付部、2 1 2 . . . 登録部、2 1 4 . . . 応答部、2 2 0 . . . 管理部、2 3 0 . . . クエリ受付部、2 3 2 . . . 検索部、2 3 4 . . . 回答部、2

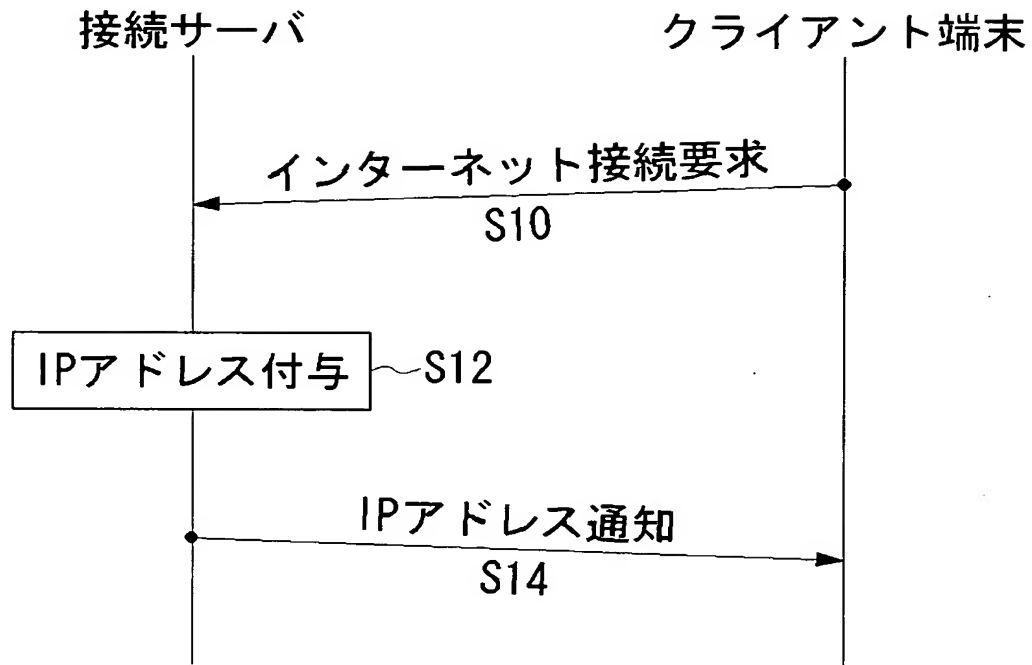
3 6 . . . マッチング管理部、2 4 0 . . . 記憶部、2 4 2 . . . ユーザデータベース、2 4 4 . . . グループデータベース、3 0 0 . . . クライアント端末、3 1 0 . . . 認証要求部、3 1 2 . . . チケット取得部、3 1 4 . . . 登録要求部、3 2 0 . . . クエリ要求部、3 2 2 . . . 回答取得部、3 3 0 . . . 通信部、3 4 0 . . . 機器 I D 保持部。

【書類名】 図面

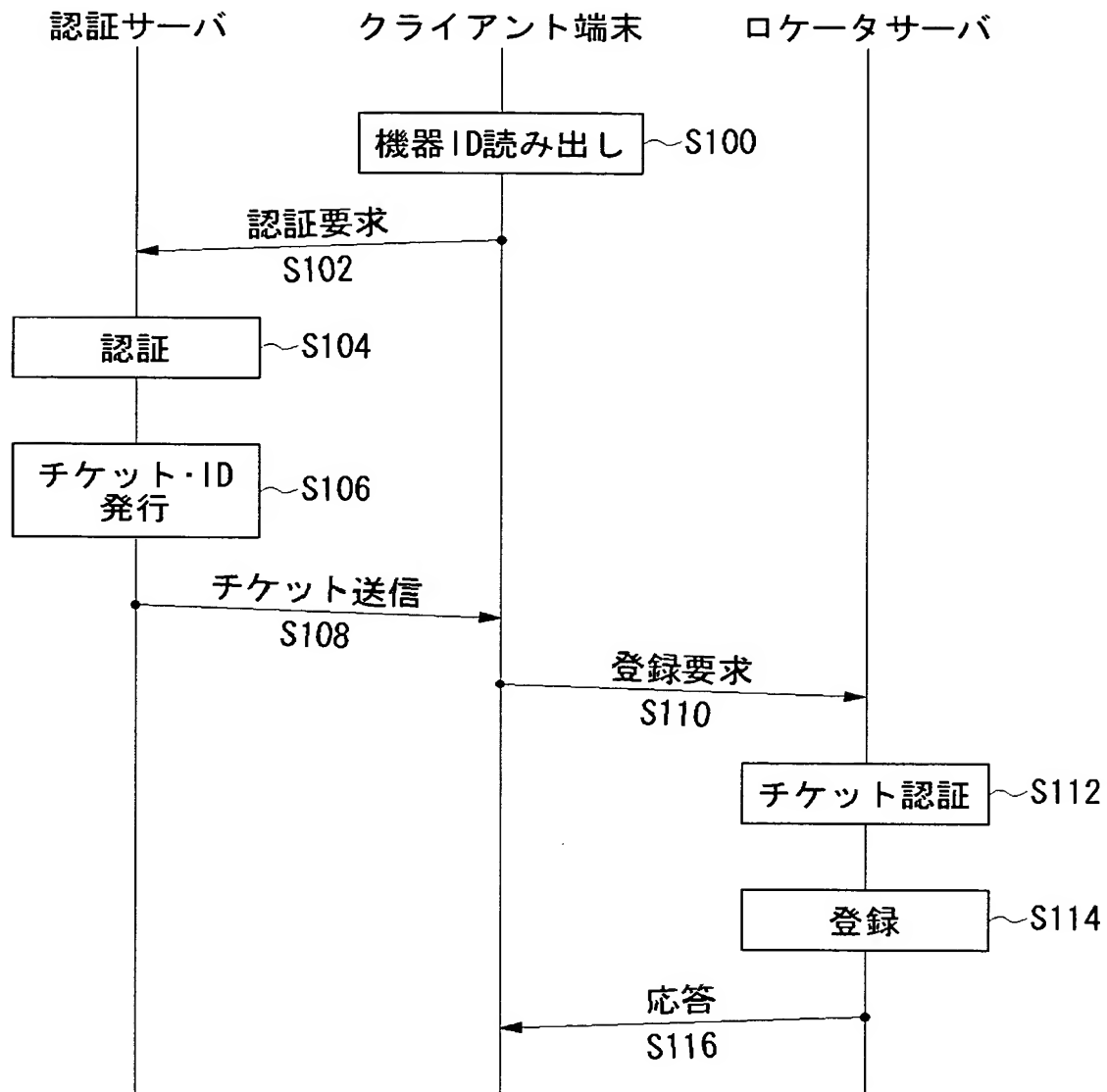
【図 1】

10

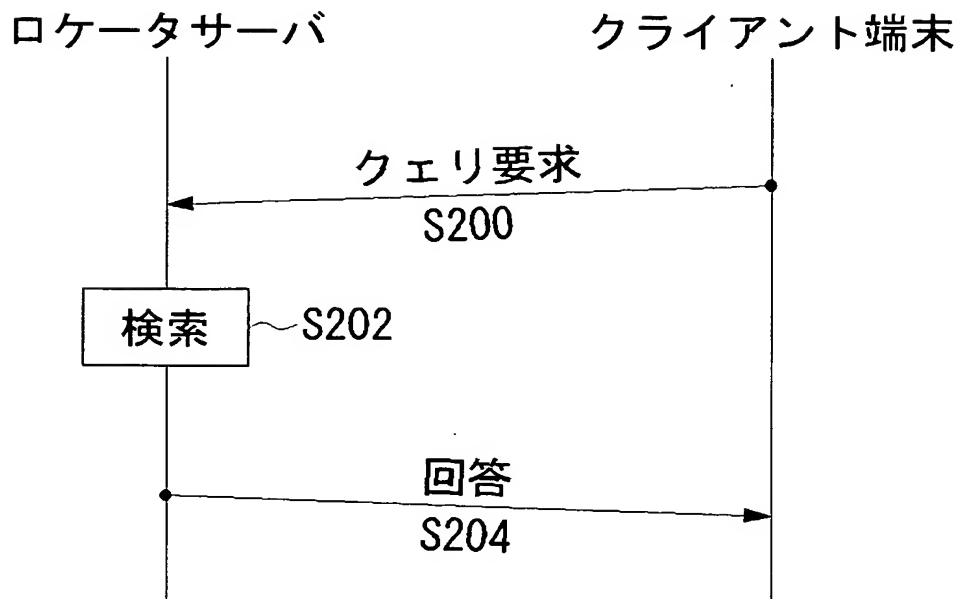
【図 2】



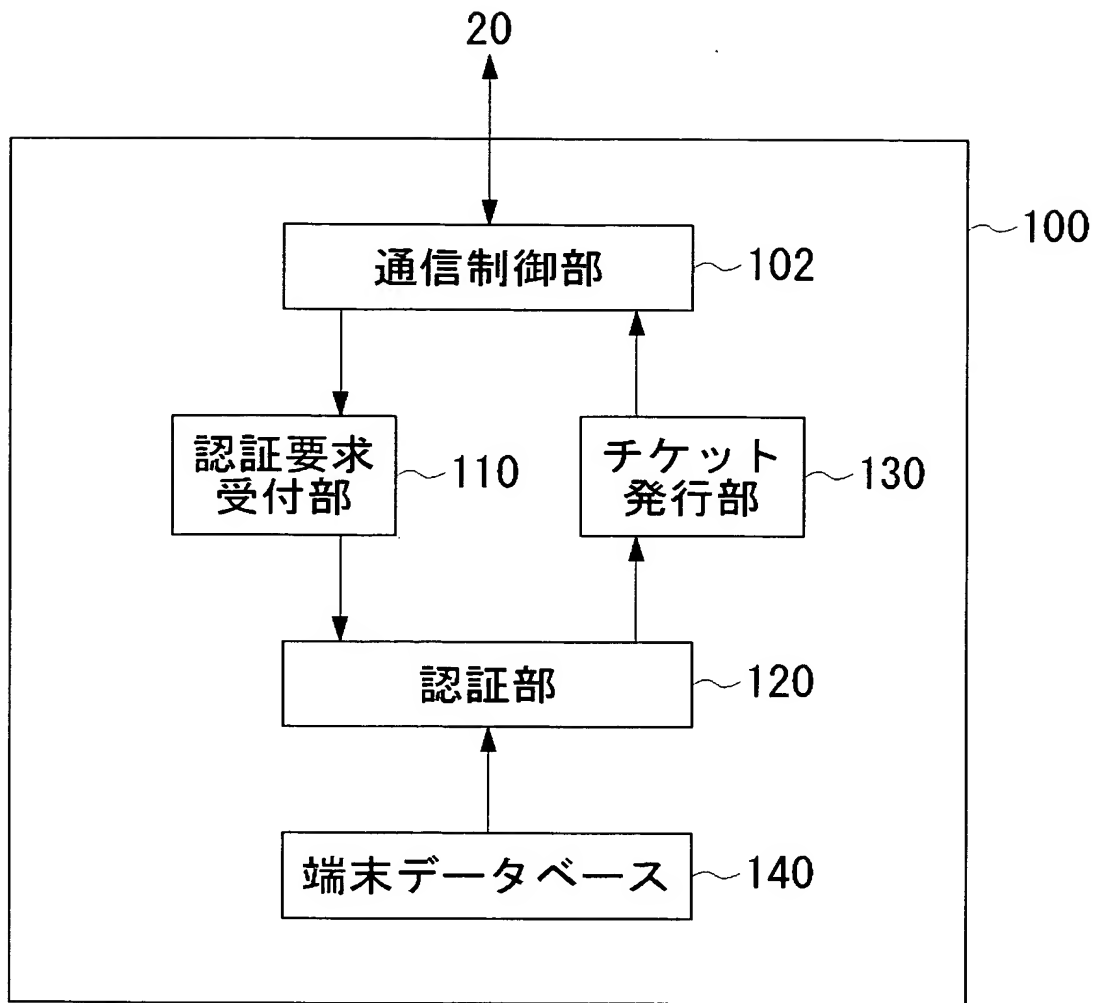
【図 3】



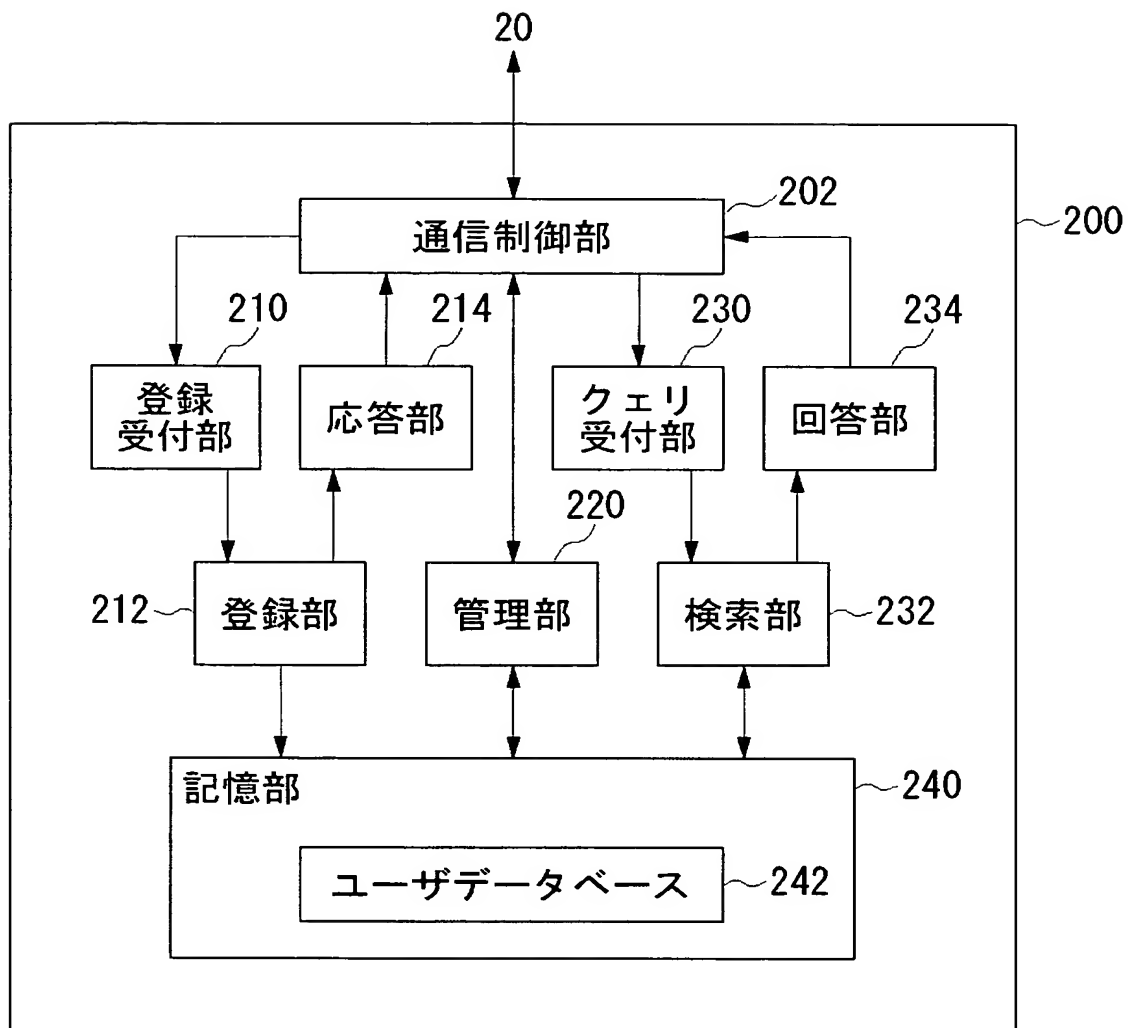
【図 4】



【図 5】



【図 6】

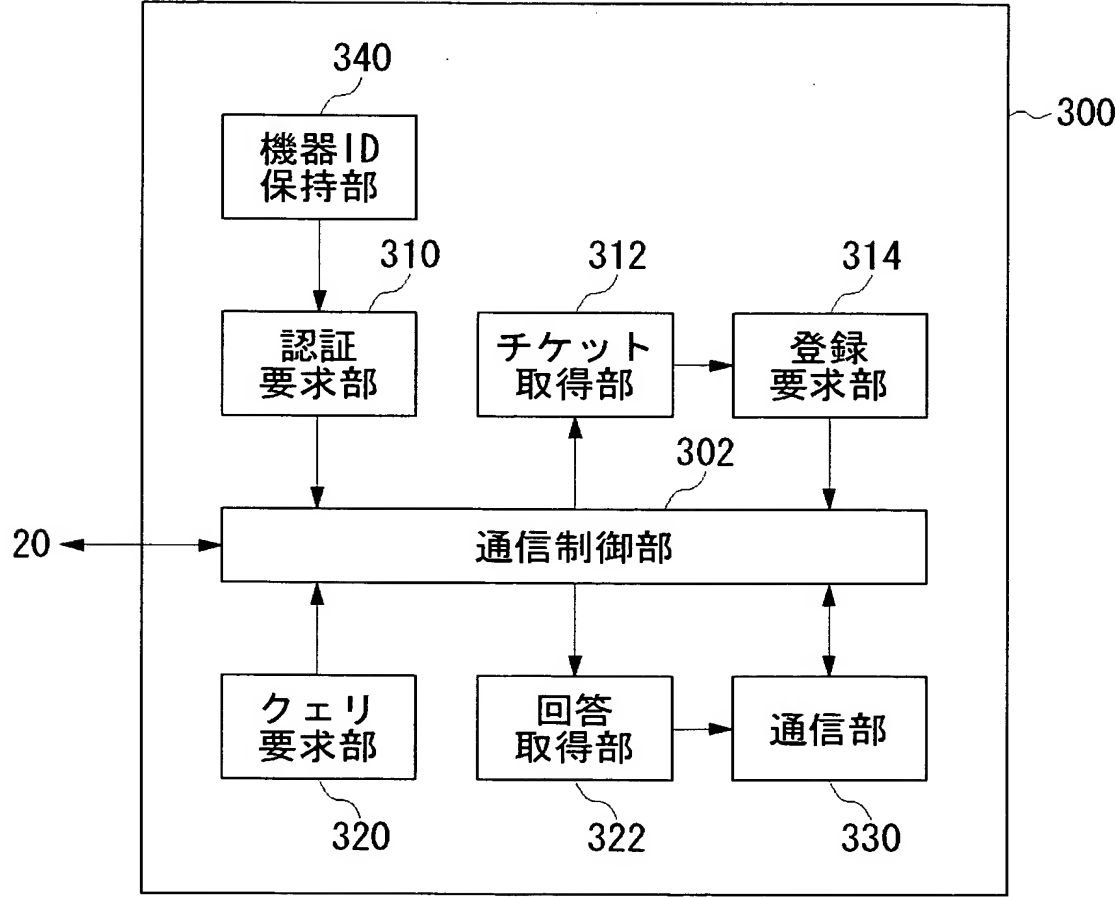


【図 7】

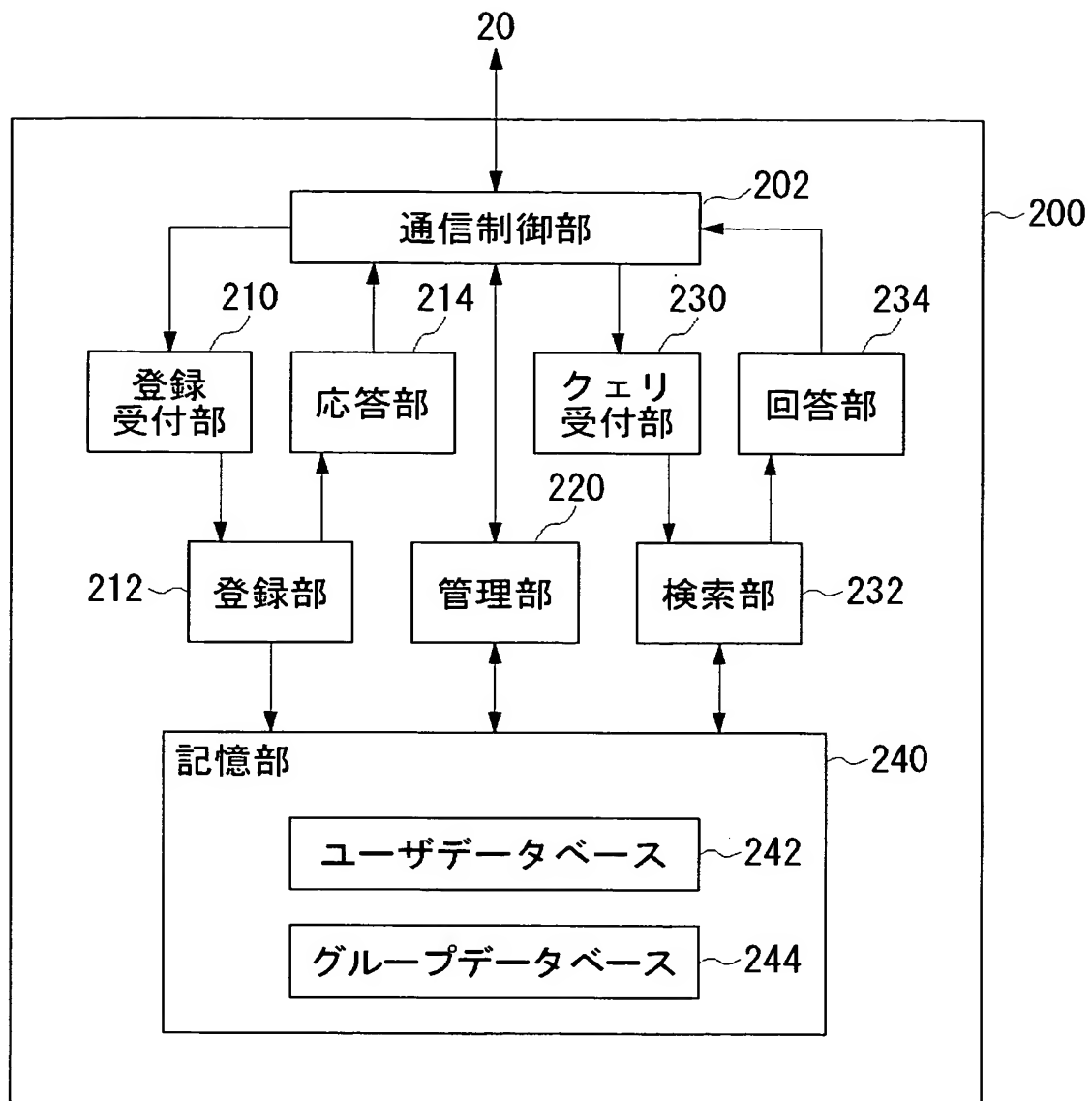
400 ロケータ ID	402 IP アドレス	404 登録日時
0001	XXX. XXX. XXX. XXX	2003/01/01 09:52:15
0002	XXX. XXX. XXX. XXX	2003/01/01 10:12:52
⋮	⋮	⋮

242

【図 8】



【図 9】



【図 1 0】

ロケータ ID	IPアドレス	登録日時	グループID
0001	XXX. XXX. XXX. XXX	2003/01/01 09:52:15	0003
0002	XXX. XXX. XXX. XXX	2003/01/01 10:12:52	—
:	:	:	:

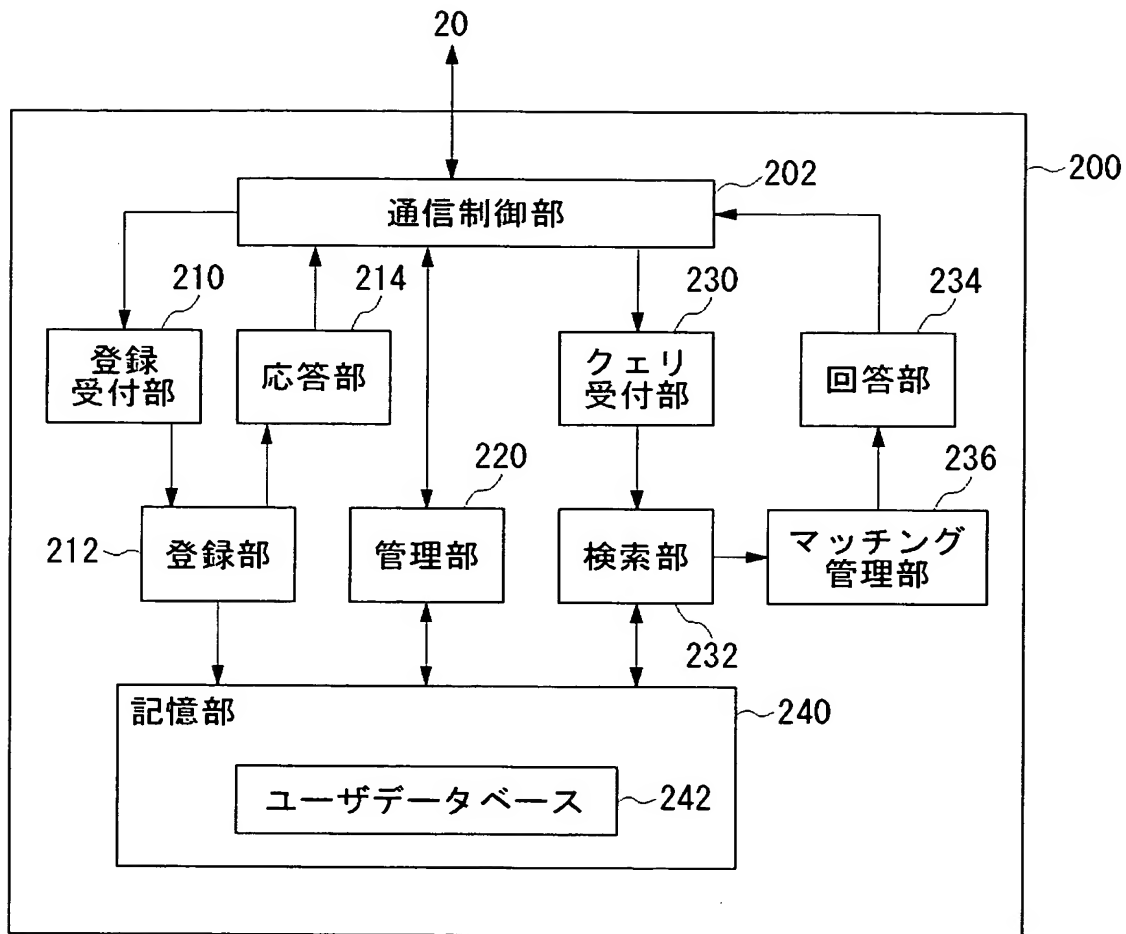
242

【図 1 1】

420	422	424	424	424	...
グループID	メンバー数	ロケータID	ロケータID	ロケータID	...
0001	2	0110	0053	—	...
0002	4	0002	1594	3258	...
:	:	:	:	:	:

244

【図 12】



【図 13】

400	402	404	406	410	412	414
ロケータID	IPアドレス	登録日時	メディアID	コミュニティ・ フラグ	ニックネーム	ネットワーク モード
0001	XXX.XXX.XXX.XXX	2003/01/01 09:52:15	525.320	1	AAA	可
0002	XXX.XXX.XXX.XXX	2003/01/01 10:12:52	072.752	4	BBB	否
:	:	:	:	:	:	:

242

【書類名】 要約書

【要約】

【課題】 ネットワークを介した端末間の通信の利便性を向上させる。

【解決手段】 クライアント端末は、自身に固定的に割り当てられている機器 ID を読み出し（S 1 0 0）、その機器 ID を認証サーバに送信して、認証を要求する（S 1 0 2）。認証サーバは、クライアント端末から受け付けた機器 ID を認証し（S 1 0 4）、認証に成功するとチケットを発行して（S 1 0 6）、クライアント端末に送信する（S 1 0 8）。クライアント端末は、チケットを受け取ると、それをロケータサーバに送信して、IP アドレスの登録を要求する（S 1 1 0）。ロケータサーバは、受け付けたチケットの正当性を検証し（S 1 1 2）、正当であることを確認すると、クライアント端末の ID と IP アドレスを対応づけて登録し（S 1 1 4）、登録が行われた旨を応答する（S 1 1 6）。

【選択図】 図 3

特願 2 0 0 3 - 1 1 3 8 4 4

出 願 人 履 歴 情 報

識別番号 [3 9 5 0 1 5 3 1 9]

1. 変更年月日 1 9 9 7 年 3 月 3 1 日
[変更理由] 住所変更
住 所 東京都港区赤坂 7 - 1 - 1
氏 名 株式会社ソニー・コンピュータエンタテインメント

2. 変更年月日 2 0 0 3 年 7 月 1 日
[変更理由] 住所変更
住 所 東京都港区南青山二丁目 6 番 2 1 号
氏 名 株式会社ソニー・コンピュータエンタテインメント